

Multivariate ultrametric root counting

Martín Avendaño, Ashraf Ibrahim

July 7, 2011

Abstract

Let K be a field, complete with respect to a discrete non-archimedean valuation and let k be the residue field. Consider a system F of n polynomial equations in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Our first result is a reformulation of the classical Hensel's Lemma in the language of tropical geometry: we show sufficient conditions (semiregularity at w) that guarantee that the first digit map $\delta: (K^*)^n \rightarrow (k^*)^n$ is a one to one correspondence between the solutions of F in $(K^*)^n$ with valuation w and the solutions in $(k^*)^n$ of the initial form system $\text{in}_w(F)$. Using this result, we provide an explicit formula for the number of solutions in $(K^*)^n$ of a certain class of systems of polynomial equations (called regular), characterized by having finite tropical prevariety, by having initial forms consisting only of binomials, and by being semiregular at any point in the tropical prevariety. Finally, as a consequence of the root counting formula, we obtain the expected number of roots in (K^*) of univariate polynomials with given support and random coefficients.

1 Introduction

The problem of counting the number of roots of univariate polynomials has been studied for at least 400 years. The first result that we point out here, stated by Descartes in 1637 [7], says that the number of positive roots (counted with multiplicities) of a nonzero polynomial $f \in \mathbb{R}[x]$ is bounded by the number of sign alternations in the sequence of coefficients of f . Over the reals, the problem of root counting was finally solved by Sturm in 1829, who gave a simple algebraic procedure to determine the exact (as opposed to an upper bound) number of real roots of a polynomial f in a given interval $[a, b]$. The problem was considered settled for many years until a interest in sparse polynomials began to grow. While Sturm's technique can count the exact number of roots of any polynomial, it is highly inefficient for polynomials of high degree with only a few nonzero terms, and also failed to provide any insight on the roots of such polynomials. On the other hand, Descartes' rule seems to be more natural for highly sparse polynomials: a simple consequence of the rule is that the number of nonzero real roots of a polynomial is bounded by twice the number of its nonzero terms. Incidentally, it has been discovered recently (see [1]) how to make Descartes' rule count the exact number of real roots: the trick is to multiply the polynomial by a high enough power of $x + 1$ before counting the sign alternations. Unfortunately, this procedure destroys completely the sparseness of the input polynomial.

In our search for a similar result over different fields, we decided to focus our attention to complete fields with respect to a non-archimedean valuation. There were several results in this setting that

indicate that an efficient root counting technique was feasible for these fields. The first of those results, obtained by H.W. Lenstra in 1999 [10], gives an upper bound for the number of nonzero roots in \mathbb{Q}_p (the field of p -adic numbers) of a polynomial $f \in \mathbb{Q}_p[x]$ as a function of the number of nonzero terms of f . The second, obtained by B. Poonen in 1998 [11], gives a similar bound over $\mathbb{F}_p((u))$ (the field of formal Laurent series with coefficients in \mathbb{F}_p). Using a more unifying approach, more of these upper bounds for ordered fields, finite extensions of \mathbb{Q}_p , and Laurent series with coefficients in fields of characteristic zero, were obtained by M. Avendaño and T. Krick in 2011 [3].

In a previous paper (see [2]), we showed a root counting procedure for univariate polynomials that do not destroy the sparsity of the given polynomial. The technique uses a combination of Hensel's Lemma and Newton Polygon to reduce root counting to solving binomials over the residue field. The only drawback of this result is that it works only with regular polynomials, which is an extensive class of polynomials defined in that paper, but not for generic polynomials in the usual sense. In this paper, we succeeded to extend those results (root counting procedure and upper bounds) to the multivariate setting, to provide a better understanding of the size of the class of regular polynomials, and also estimates for the expected number of zeros of random sparse polynomials. Our counting procedure uses basic tropical geometry and a multivariate version of Hensel's Lemma to reduce the problem to solving binomial square systems over the residue field.

Our bound for the number of zeros of sparse multivariate square system of polynomials should be compared with the bound obtained by J.M. Rojas in 2004 [14], which can be regarded as the p -adic counterpart of A. Khovanskii's theorem for fewnomials over the reals [9], or as the extension of Lenstra's estimates in the univariate case [10]. Rojas showed that, over any finite extension K/\mathbb{Q}_p , any such system of polynomials has at most $1 + (C_K n(t-n)^3 \log(t-n))^n$ zeros, where t is the total number of different exponents vectors appearing in polynomials and C_K is a computable constant that depends only on K . Our counting gives a stronger bound, although only for regular systems:

Theorem 1.1. *Let $F = (f_1, \dots, f_n)$ be a regular¹ system of polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Assume that the residue field k is finite. Then the number of zeros of F in $(K^*)^n$ is at most $\binom{t_1}{2} \cdots \binom{t_n}{2} |k^*|^n$, where t_i is the number of nonzero monomials of f_i .*

This represents an improvement from roughly t^{3n} to t^{2n} in the case of regular systems.

Let K be a complete field with respect to a discrete non-archimedean valuation $v : K \rightarrow \mathbb{R} \cup \{\infty\}$. Let $A = \{x \in K : v(x) \geq 0\}$ be the valuation ring of K . The ring A is local with maximal ideal $\mathfrak{M} = \{x \in K : v(x) > 0\}$, which is principal $\mathfrak{M} = \pi A$ since v is discrete. We denote by $k = A/\mathfrak{M}$ the residue field of K with respect to v . We denote the first digit of $x \in K^*$ by $\delta(x) = \pi^{-v(x)/v(\pi)} x \bmod \mathfrak{M}$. The map $\delta : K^* \rightarrow k^*$ is a homomorphism, that can be seen as the composition of the homomorphisms

$$K^* \rightarrow \mathbb{Z} \times A^* \rightarrow A^* \rightarrow k^*,$$

where the first map is the isomorphism $x \mapsto (v(x)/v(\pi), \pi^{-v(x)/v(\pi)} x)$, the second arrow is the projection on the second factor, and the third arrow is the reduction modulo \mathfrak{M} .

¹see definition 4.1.

Fix a set $\Delta \subseteq A \setminus \mathfrak{M}$ of representatives of the first digit map. For any $x \in K^*$, we write $\Delta(x)$ the representative corresponding to $\delta(x)$. Any element in $x \in K^*$ can be factorized as $x = \pi^{v(x)/v(\pi)} \Delta(x) e(x)$ where $e(x) = x \pi^{-v(x)/v(\pi)} \Delta(x)^{-1} \in 1 + \mathfrak{M}$. Moreover, this is the only possible factorization of x as the product of a power of π , an element in Δ , and an element in $1 + \mathfrak{M}$. This implies that the map $K^* \rightarrow v(\pi)\mathbb{Z} \times k^* \times (1 + \mathfrak{M})$ given by $x \mapsto (v(x), \delta(x), e(x))$ is a bijection. The spirit behind most of our results is this bijection: we compute/count the solutions of systems of polynomials by first looking at the valuation, then the first digit, and then the tail in $1 + \mathfrak{M}$. Our notions of genericity and randomness are also based on the bijection.

Consider a square system $F = (f_1, \dots, f_n)$ of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Denote by $Z_K(F)$ the set of solutions of F in $(K^*)^n$. The study of the set $Z_K(F)$ that we do in this paper is based on the following program:

1. Study the set $S(F) = \{v(x) : x \in Z_K(F)\} \subseteq v(\pi)\mathbb{Z}^n$.

2. For each $w \in S(F)$ study the set

$$D_w(F) = \{\delta(x) : x \in Z_K(F), v(x) = w\} \subseteq (k^*)^n.$$

3. For each $w \in S(F)$ and $\varepsilon \in D_w(F)$ study the set

$$E_{w,\varepsilon}(F) = \{e(x) : x \in Z_K(F), v(x) = w, \delta(x) = \varepsilon\} \subseteq (1 + \mathfrak{M})^n.$$

A similar program was successfully used by B. Sturmfels and D. Speyer in [15], working on the field of Puiseux series $\mathbb{C}\{\{t\}\}$, to give a simple proof of Kapranov's Theorem: item 1 correspond with their Theorem 2.1 and item 2 with Corollary 2.2.

Our approach for the first problem requires us to work only with the valuations of the coefficients and the exponent vectors of the monomials of F . We will prove that $S(F) \subseteq \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$, where the set $\text{Trop}(F) = \text{Trop}(f_1) \cap \dots \cap \text{Trop}(f_n)$ is the tropical prevariety induced by F . Recall that for a given polynomial $f = \sum_{i=1}^t a_i X^{\alpha_i} \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$, the set $\text{Trop}(f)$ is defined as the set of all possible $w \in \mathbb{R}^n$ such that $v(a_i) + w \cdot \alpha_i$ for $i = 1, \dots, t$ reaches its minimum value at least twice. For any $w \in \mathbb{R}^n$, the initial form $\text{in}_w(f) \in k[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ is defined as the sum of $\delta(a_i) X^{\alpha_i}$, but including only the terms that minimize $v(a_i) + w \cdot \alpha_i$. All the notions of tropical geometry used in this paper are defined in Section 2 and can also be found in the literature in [15, 12, 6].

For the second problem, we introduce the notion of w -semiregularity at a given $w \in \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$, that guarantees that $D_w(F)$ coincides with the set of zeros of the initial form system $\text{in}_w(F)$ in $(k^*)^n$. In a few words, semiregularity at w is a condition on F that reformulates the hypothesis of Hensel's Lemma (see [13, Pag. 48]) for zeros of valuation w and for polynomials with coefficients in K instead of A . Semiregularity at w also provides the solution of the third problem: for each $w \in \text{Trop}(F)$ and $\varepsilon \in D_w(F)$, there is exactly one solution of F in $(K^*)^n$ with valuation vector w and first digits ε , i.e. the set $E_{w,\varepsilon}(F)$ has only one element. In particular, for a w -semiregular system of polynomials F , where $w \in \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$, the first digit map $\delta : (K^*)^n \rightarrow (k^*)^n$ provides a bijection between roots of F with valuation w and roots of the initial form system $\text{in}_w(F)$ in $(k^*)^n$.

The definition of semiregularity (that was obtained by keeping track several changes of variables carefully) and the main root counting theorem (proven by undoing all these changes of variables) are presented in detail in Section 3 and summarized in the following statement:

Theorem 1.2. *Let $F = (f_1, \dots, f_n)$ be a system of polynomial equations in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $w \in v(\pi)\mathbb{Z}^n$ be an isolated point of $\text{Trop}(F)$. If the initial form system $\text{in}_w(F)$ has no degenerate zeros in $(k^*)^n$, then the first digit map induces a bijection between the set of zeros of F in $(K^*)^n$ with valuation w and the set of zeros of $\text{in}_w(F)$ in $(k^*)^n$.*

As a consequence of the results described in the last paragraph, we derive explicit formulas (or more precisely, an algorithm) to compute efficiently the number of roots in $(K^*)^n$ of a large class of systems of polynomial equations. These systems, called regular, are characterized by having a finite tropical prevariety, by being semiregular at any point, and by having initial forms consisting only of binomials. Our notion of regularity and the formulas for the number of roots generalize those shown in [2, Def. 1, Thm. 4.5] to the multivariate case. All this work is done in Section 4.

Although regularity seems to impose a very strong constraint on the system, we prove in Section 5 that this is not actually the case: regularity occurs generically when the residue field k has characteristic zero. The notion of genericity implicit in the previous statement (called tropical genericity) refers to coefficients whose valuation vector do not lie in the union of certain hyperplanes. This notion is the natural extension of the genericity in the algebraic geometry sense to tropical geometry.

Since we have explicit formulas for the number of roots of generic polynomials (with given support), we should be able to compute the expected number of roots in $(K^*)^n$ of random polynomials. The only problem is that we need a way of choosing the coefficients at random that produce tropically generic systems with probability 1. Since our root counting formula does not depend on the tail in $1 + \mathfrak{M}$ of the coefficients, we only need a way of selecting the valuation of the coefficients and their first digits. The approach that we use consists of choosing the valuation at random uniformly in an interval $[-M, M]$ and then letting M go to infinity. The first digits are selected uniformly from k^* when k is a finite field, or in the case of $k = \mathbb{R}$ with any probability measure that gives equal probability to $\mathbb{R}_{>0}$ and $\mathbb{R}_{<0}$. In the case that k is algebraically closed, any selection of the first digits gives the same number of roots, and therefore no probability measure in k is needed.

Let $\mathcal{A} = \{\alpha_1 < \alpha_2 < \dots < \alpha_t\} \subset \mathbb{Z}$ be a finite set ($t \geq 2$) and consider an univariate polynomial $f \in K[X]$ with $\text{supp}(f) = \mathcal{A}$ and random coefficients (chosen as explained above). Let $E(\mathcal{A}, K)$ be the limit of the expected number of roots of f in K^* as M goes to infinity. Our main result of section 6, is a general formula for $E(\mathcal{A}, K)$. As a particular case, we have the following result that it is interesting in itself, and simple enough to be stated in this introduction:

Theorem 1.3. *Let $\mathcal{A} = \{\alpha_1 < \alpha_2 < \dots < \alpha_t\} \subset \mathbb{Z}$ be a finite set with $t \geq 2$. If k is algebraically closed with $\text{char}(k) = 0$ or $\text{char}(k) > \max_{\alpha, \beta \in \mathcal{A}} |\alpha - \beta|$, then*

$$2 - \frac{2}{t} \leq E(\mathcal{A}, K) \leq 2 \ln(t).$$

A previous estimation for the expected number of roots of random polynomials with p -adic coefficients, although for a different distribution (related to the Haar measure on \mathbb{Z}_p) was obtained by S. Evans in [8].

2 Tropical hypersurface induced by a Laurent polynomial

The main goal of this section is to introduce the reader the notions of tropical geometry used in the rest of the paper.

Definition 2.1. Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ be a polynomial with t non-zero terms $f = \sum_{i=1}^t a_i X^{\alpha_i}$ where $a_i \in K^*$ and $\alpha_i = (\alpha_{i1}, \dots, \alpha_{in}) \in \mathbb{Z}^n$ for all $i = 1, \dots, t$. We define the tropicalization of f as the piecewise linear function $\text{tr}(f; w) = \min\{l_i(f; w) \mid i = 1, \dots, t\}$ where $l_i(f; w) = v(a_i) + \alpha_i \cdot w$. The tropical hypersurface induced by f is the set

$$\text{Trop}(f) = \{w_0 \in \mathbb{R}^n : \text{tr}(f; w) \text{ is not differentiable at } w_0\}.$$

The value of $l_i(f; w)$ is usually referred in the literature as the w -weight of the i -th term of f .

Lemma 2.2. Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ be a polynomial with t terms and let $w_0 \in \mathbb{R}^n$. Then $w_0 \in \text{Trop}(f)$ if and only if there are indices $1 \leq i < j \leq t$ such that $l_i(f; w_0) = l_j(f; w_0) \leq l_k(f; w_0)$ for all $k = 1, \dots, t$.

Proof. (\Leftarrow) Assume first that $l_i(f; w_0) < l_k(f; w_0)$ for all $k \neq i$. Since the functions $l_i(f; w)$ are continuous, all these inequalities remain valid in a neighborhood U of w_0 , and then $\text{tr}(f; w)$ coincides with the linear function $l_i(f; w)$ in U . In particular, $\text{tr}(f; w)$ is differentiable at w_0 , i.e. $w_0 \notin \text{Trop}(f)$. (\Rightarrow) Now take $w_0 \in \text{Trop}(f)$. Since $\text{tr}(f; w)$ is differentiable at w_0 , then the linear function $l(w) = \text{tr}(f; w_0) + \nabla \text{tr}(f; w_0) \cdot (w - w_0)$ approximates $\text{tr}(f; w)$ with order two near w_0 , and since $\text{tr}(f; w)$ is piecewise linear, then $\text{tr}(f; w) = l(w) = l_i(f; w)$ for some $1 \leq i \leq t$ in a neighborhood U of w_0 . Therefore, for any other index $k \neq i$, we have that $\text{tr}(f; w) = l_i(f; w) \leq l_k(f; w)$ in U , or equivalently, $l_i(f; w_0) - l_k(f; w_0) \leq (\alpha_k - \alpha_i) \cdot (w - w_0)$ in U . The right hand side of this inequality can be made strictly negative by selecting $w - w_0$ a vector with the direction of $\alpha_i - \alpha_k$, hence $l_i(f; w_0) < l_k(f; w_0)$ for all $k \neq i$. \square

Note that for any $x \in (K^*)^n$, the valuation of the i -th term of f at x is given by $l_i(f; v(x))$.

Proposition 2.3. Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and let $x \in (K^*)^n$ be a zero of f . Then $v(x) \in \text{Trop}(f)$.

Proof. Sort all the t monomials of f according to their valuation at x .

$$l_{i_1}(f; v(x)) \leq l_{i_2}(f; v(x)) \leq \dots \leq l_{i_t}(f; v(x))$$

Since the sum of all the monomials at x is zero, the first two valuations in this list must coincide. We conclude from Lemma 2.2 that $v(x) \in \text{Trop}(f)$. \square

Definition 2.4. Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ be a polynomial with t non-zero terms $f = \sum_{i=1}^t a_i X^{\alpha_i}$ and let $w \in \mathbb{R}^n$. We define the lower polynomial $f^{[w]}$ of f with respect to the valuation vector w as

$$f^{[w]} = \sum_{i : l_i(f; w) = \text{tr}(f; w)} a_i X^{\alpha_i} \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}].$$

We also define the initial form $\text{in}_w(f)$ of f with respect to w as

$$\text{in}_w(f) = \sum_{i : l_i(f; w) = \text{tr}(f; w)} \delta(a_i) X^{\alpha_i} \in k[X_1^{\pm 1}, \dots, X_n^{\pm 1}].$$

Note that, according to Lemma 2.2, $w \in \text{Trop}(f)$ if and only if $\text{in}_w(f)$ has at least two terms. This can be taken as an alternative definition of the tropical hypersurface. A key property of the initial forms is that if $x \in (K^*)^n$ is a solution of f with $v(x) = w$, then $\delta(x) \in (k^*)^n$ is a solution of $\text{in}_w(f)$, as shown in the following lemma.

Lemma 2.5. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$, let $w \in \mathbb{R}^n$, let $x \in (K^*)^n$ with $v(x) = w$, and let $1 \leq j \leq n$. Then:*

1. $\pi^{-\text{tr}(f;w)/v(\pi)} f(x) \in A$.
2. $\pi^{-\text{tr}(f;w)/v(\pi)} f(x) \equiv \text{in}_w(f)(\delta(x)) \pmod{\mathfrak{M}}$.
3. $\pi^{(w_j - \text{tr}(f;w))/v(\pi)} \frac{\partial f}{\partial X_j}(x) \in A$.
4. $\pi^{(w_j - \text{tr}(f;w))/v(\pi)} \frac{\partial f}{\partial X_j}(x) \equiv \frac{\partial \text{in}_w(f)}{\partial X_j}(\delta(x)) \pmod{\mathfrak{M}}$.

Proof. Let $f = \sum_{i=1}^t a_i X^{\alpha_i} \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. The valuation of the i -th term of $f(x)$ is $l_i(f; w)$ and the minimum of all these valuations is $\text{tr}(f; w)$. This proves that $\pi^{-\text{tr}(f;w)/v(\pi)} f(x) \in A$. Moreover, if $l_i(f; w) > \text{tr}(f; w)$, then the i -term of $f(x)$ multiplied by $\pi^{-\text{tr}(f;w)/v(\pi)}$ reduces to zero modulo \mathfrak{M} , so $\pi^{-\text{tr}(f;w)/v(\pi)} f(x) \equiv \pi^{-\text{tr}(f;w)/v(\pi)} f^{[w]}(x) \pmod{\mathfrak{M}}$. Besides, all the terms in $\pi^{-\text{tr}(f;w)/v(\pi)} f^{[w]}(x)$ have valuation zero, so reducing it modulo \mathfrak{M} is the same as adding the first digit of each term. This proves that $\pi^{-\text{tr}(f;w)/v(\pi)} f(x) \equiv \text{in}_w(f)(\delta(x)) \pmod{\mathfrak{M}}$. The partial derivative of f with respect to X_j is $\partial f / \partial X_j = \sum_{i=1}^t a_i \alpha_{i,j} X^{\alpha_i - e_j}$, where $\{e_1, \dots, e_n\}$ is the standard basis of \mathbb{R}^n . The valuation of the i -th term of $\partial f / \partial X_j(x)$ is $l_i(f; w) - w_j + v(\alpha_{i,j})$, thus $\pi^{(w_j - \text{tr}(f;w))/v(\pi)} \partial f / \partial X_j(x) \in A$. Finally, in the reduction of $\pi^{(w_j - \text{tr}(f;w))/v(\pi)} \partial f / \partial X_j(x)$ modulo \mathfrak{M} , all the terms with $l_i(f; w) > \text{tr}(f; w) - w_j$ disappear, as well as the terms with $v(\alpha_{i,j}) > 0$. The remaining terms have all valuation zero, and their first digits coincide with those of $\partial \text{in}_w(f) / \partial X_j(\delta(x))$. \square

The following lemma shows that the notions of tropicalization, tropical hypersurface, lower polynomial, and initial form, behave well under rescaling of the variables and multiplication by monomials.

Lemma 2.6. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$, $a \in K^*$, $b = (b_1, \dots, b_n) \in (K^*)^n$, $\alpha \in \mathbb{Z}^n$ and $w \in \mathbb{R}^n$.*

1. $\text{tr}(aX^\alpha f; w) = \text{tr}(f; w) + v(a) + \alpha \cdot w$.
2. $\text{Trop}(aX^\alpha f) = \text{Trop}(f)$.
3. $(aX^\alpha f)^{[w]} = aX^\alpha f^{[w]}$.
4. $\text{in}_w(aX^\alpha f) = \delta(a)X^\alpha \text{in}_w(f)$.
5. $\text{tr}(f(b_1 X_1, \dots, b_n X_n); w) = \text{tr}(f; w + v(b))$.
6. $\text{Trop}(f(b_1 X_1, \dots, b_n X_n)) = \text{Trop}(f) - (v(b_1), \dots, v(b_n))$.
7. $f(b_1 X_1, \dots, b_n X_n)^{[w]} = f^{[w+v(b)]}(b_1 X_1, \dots, b_n X_n)$.
8. $\text{in}_w(f(b_1 X_1, \dots, b_n X_n)) = \text{in}_{w+v(b)}(f)(\delta(b_1)X_1, \dots, \delta(b_n)X_n)$.

Proof. Items 1 and 5 follow immediately from the identities $l_i(aX^\alpha f; w) = l_i(f; w) + v(a) + \alpha \cdot w$ and $l_i(f(b_1X_1, \dots, b_nX_n); w) = l_i(f; w + v(b))$. Items 2 and 6 are consequences of the previous two and the definition of tropical hypersurface. The indices of the monomials of f that are in $(aX^\alpha f)^{[w]}$ correspond with the indices that minimize the value of $l_i(aX^\alpha f; w)$. Since $v(a) + \alpha \cdot w$ is a constant, these indices also minimize $l_i(f; w)$, i.e. they correspond with the monomials of f in $f^{[w]}$. Therefore $(aX^\alpha f)^{[w]} = aX^\alpha f^{[w]}$. Similarly, the indices of the terms of f in $f(b_1X_1, \dots, b_nX_n)^{[w]}$ minimize the expression $l_i(f(b_1X_1, \dots, b_nX_n); w)$, and therefore, coincide with the same indices of the monomials in $f^{[w+v(b)]}(b_1X_1, \dots, b_nX_n)$. This proves that $f(b_1X_1, \dots, b_nX_n)^{[w]} = f^{[w+v(b)]}(b_1X_1, \dots, b_nX_n)$. Finally, items 4 and 8 follow from 3 and 7 by taking the first digit of all the terms. \square

In the next two lemmas, we show the relation between $\text{Trop}(f)$ and $\text{Trop}(f^{[w]})$ for any $w \in \mathbb{R}^n$. It is clear that if $w \notin \text{Trop}(f)$, then $f^{[w]}$ is a single monomial, and therefore $\text{Trop}(f^{[w]}) = \emptyset$. Otherwise, when $w \in \text{Trop}(f)$, we have $w \in \text{Trop}(f^{[w]})$ and $\text{tr}(f; w) = \text{tr}(f^{[w]}; w)$. We will prove next that the tropical hypersurface $\text{Trop}(f^{[w]})$ is a cone centered at w , that coincides with $\text{Trop}(f)$ in a neighborhood of w . This completely characterizes $\text{Trop}(f^{[w]})$ in terms of $\text{Trop}(f)$.

Lemma 2.7. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and let $w \in \text{Trop}(f)$. Then, for any $w' \in \text{Trop}(f^{[w]})$, the ray $w + \lambda(w' - w)$ with $\lambda \geq 0$ is contained in $\text{Trop}(f^{[w]})$.*

Proof. Let t be the number of terms of f . Write the lower polynomial of f at w as $f^{[w]} = a_{i_1}X^{\alpha_{i_1}} + \dots + a_{i_r}X^{\alpha_{i_r}}$ where $1 \leq i_1 < i_2 < \dots < i_r \leq t$ are all the indices that minimize the linear functions $l_i(f; w)$. The s -th term of $f^{[w]}$ is the i_s -th term of f . In particular, we have that $l_s(f^{[w]}; w) = l_{i_s}(f; w) = \text{tr}(f; w)$ for all $s = 1, \dots, r$. Since $w' \in \text{Trop}(f^{[w]})$ we have, by Lemma 2.2, two indices $1 \leq n < m \leq r$ such that $l_n(f^{[w]}; w') = l_m(f^{[w]}; w') \leq l_s(f^{[w]}; w')$ for all $s = 1, \dots, r$. Subtracting $\text{tr}(f; w)$, multiplying by $\lambda \geq 0$ and then adding $\text{tr}(f; w)$ to these (in)equalities we get

$$l_n(f^{[w]}; w + \lambda(w' - w)) = l_m(f^{[w]}; w + \lambda(w' - w)) \leq l_s(f^{[w]}; w + \lambda(w' - w))$$

for all $s = 1, \dots, r$. This implies, by Lemma 2.2, that $w + \lambda(w' - w)$ is in $\text{Trop}(f^{[w]})$. \square

Lemma 2.8. *Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and let $w \in \text{Trop}(f)$. Then there exists $\varepsilon > 0$ such that $\text{Trop}(f) \cap B_\varepsilon(w) = \text{Trop}(f^{[w]}) \cap B_\varepsilon(w)$.*

Proof. Let t be the number of terms of f . Let $I = \{1 \leq i \leq t : l_i(f; w) = \text{tr}(f; w)\}$ be the set of indices of the monomials of f in $f^{[w]}$. Note that $l_i(f; w) < l_k(f; w)$ for all $i \in I$ and $k \notin I$. Since $l_i(f; \cdot) : \mathbb{R}^n \rightarrow \mathbb{R}$ are continuous functions, there exists $\varepsilon > 0$ such that

$$l_i(f; w') < l_k(f; w') \quad \forall w' \in B_\varepsilon(w), \forall i \in I, \forall k \notin I. \quad (1)$$

Take $w' \in \text{Trop}(f) \cap B_\varepsilon(w)$. By Lemma 2.2, there are indices $1 \leq i < j \leq t$ such that $l_i(f; w') = l_j(f; w') \leq l_k(f; w')$ for all $k = 1, \dots, t$. By the inequalities (1), we conclude that $i, j \in I$. Therefore, by Lemma 2.2, $w' \in \text{Trop}(f^{[w]})$.

Now take $w' \in \text{Trop}(f^{[w]}) \cap B_\varepsilon(w)$. By Lemma 2.2 we have two different indices $i, j \in I$ such that $l_i(f; w') = l_j(f; w') \leq l_k(f; w')$ for all $k \in I$. By (1), this inequality holds also for $k \notin I$. This means, by Lemma 2.2, that $w' \in \text{Trop}(f)$. \square

Lemma 2.2 gives a simple procedure to compute tropical hypersurfaces that require to solve systems of linear equations and inequalities. The following is a simple geometric interpretation of that using polyhedra.

Definition 2.9. Let $f = \sum_{i=1}^t a_i X^{\alpha_i} \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. The Newton Polytope of f , denoted $\text{NP}(f)$, is the convex hull of the set

$$\{(\alpha_i, v(a_i)) : i = 1, \dots, t\} \subseteq \mathbb{R}^{n+1}.$$

A hyperplane $H \subseteq \mathbb{R}^{n+1}$, not parallel to the line $x_1 = \dots = x_n = 0$, is a supporting hyperplane of the Newton Polytope of f if $\text{NP}(f)$ is included in the upper half-space² determined by H and $\text{NP}(f) \cap H \neq \emptyset$.

Lemma 2.10. Let $f \in K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Then $\text{Trop}(f)$ is the set of all $w \in \mathbb{R}^n$ such that $(w, 1) \in \mathbb{R}^{n+1}$ is the normal vector of a supporting hyperplane H of $\text{NP}(f)$ with $|H \cap \text{NP}(f)| > 1$.

Proof. Write $f = \sum_{i=1}^t a_i X^{\alpha_i}$. (\subseteq) Take $w \in \text{Trop}(f)$. By Lemma 2.2, there are two indices $1 \leq i < j \leq t$ such that $l_i(f; w) = l_j(f; w) \leq l_k(f; w)$ for all $k = 1, \dots, t$. This is equivalent to say that the hyperplane

$$H = \{x \in \mathbb{R}^{n+1} : (w, 1) \cdot x = \text{tr}(f; w)\},$$

with normal vector $(w, 1)$, contains the points $(\alpha_i, v(a_i))$ and $(\alpha_j, v(a_j))$, and the upper half-space H^+ determined by H contains all the points $(\alpha_k, v(a_k))$. Since H^+ is convex, then $\text{NP}(f) \subseteq H^+$. (\supseteq) Now assume that H is a supporting hyperplane with normal vector $(w, 1)$ that contains at least two points of the Newton Polytope of f . Since $\text{NP}(f)$ is a polyhedron, then H contains at least two vertices $(\alpha_i, v(a_i))$ and $(\alpha_j, v(a_j))$. The remaining vertices are contained in the upper half-space determined by H . This means that $\alpha_i \cdot w + v(a_i) = \alpha_j \cdot w + v(a_j) \leq \alpha_k \cdot w + v(a_k)$ for all $k = 1, \dots, t$, and by Lemma 2.2, that $w \in \text{Trop}(f)$. \square

In the case of an univariate polynomial $f \in K[X]$, Lemma 2.10 says that $\text{Trop}(f)$ is the set of minus the slope of the segments of the lower hull of $\text{NP}(f)$.

3 Semiregular systems of polynomial equations.

Definition 3.1. Consider a system F of n equations in n variables.

$$F = \begin{cases} f_1(X_1, \dots, X_n) = 0 \\ \vdots \\ f_n(X_1, \dots, X_n) = 0 \end{cases}$$

The equations are given by non-zero polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and the unknowns are in K^* . The system F will be written (f_1, \dots, f_n) in order to simplify the notation. We define the tropical prevariety $\text{Trop}(F)$ induced by F as

$$\text{Trop}(F) = \text{Trop}(f_1) \cap \dots \cap \text{Trop}(f_n).$$

²Up and down is understood with respect to the variable x_{n+1} . The upper half-space of H is well-defined since H is not parallel to the vertical axis.

For any $w \in \text{Trop}(F)$ we denote by $F^{[w]}$ and $\text{in}_w(F)$ the systems of polynomial equations given by the lower polynomials $f_1^{[w]}, \dots, f_n^{[w]}$ and the initial forms $\text{in}_w(f_1), \dots, \text{in}_w(f_n)$ respectively.

By Proposition 2.3, any solution $x \in (K^*)^n$ of F satisfies $v(x) \in \text{Trop}(F)$.

Lemma 3.2. *Let F be a system of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. If w is an isolated point of $\text{Trop}(F)$, then $\text{Trop}(F^{[w]}) = \{w\}$ and all the solutions $x \in (K^*)^n$ of $F^{[w]}$ have valuation vector $v(x) = w$.*

Proof. By Lemma 2.8, the tropical prevarieties $\text{Trop}(F)$ and $\text{Trop}(F^{[w]})$ coincide in a neighborhood of w . In particular, there exists $\varepsilon > 0$ such that $\text{Trop}(F^{[w]}) \cap B_\varepsilon(w) = \{w\}$. On the other hand, by Lemma 2.7, the tropical prevariety $\text{Trop}(F^{[w]})$ is a cone centered at w . This implies that $\text{Trop}(F^{[w]}) = \{w\}$. Therefore, by Proposition 2.3, all the solutions $x \in (K^*)^n$ of $F^{[w]}$ have valuation vector $v(x) = w$. \square

Definition 3.3. *Consider a system $F = (f_1, \dots, f_n)$ of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$, and let $w \in \mathbb{R}^n$. We say that F is semiregular at w if either $w \notin \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$ or $\text{in}_w(F)$ has no degenerate zero in $(k^*)^n$. We say that F is normalized at w if $\text{tr}(f_1; w) = \dots = \text{tr}(f_n; w) = 0$.*

Lemma 3.4. *Let $F = (f_1, \dots, f_n)$ be a system of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ semiregular at $w \in \mathbb{R}^n$. Then, for each zero $x \in (K^*)^n$ of F with $v(x) = w$, we have*

$$v(\text{Jac}(F)(x)) = \text{tr}(f_1; w) + \dots + \text{tr}(f_n; w) - (w_1 + \dots + w_n).$$

Proof. In the case $w \notin \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$, there are no zeros of F with valuation w , and there is nothing to prove. Therefore, we can assume without loss of generality that $w \in \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$. Take a zero $x \in (K^*)^n$ of F with valuation $v(x) = w$. By Lemma 2.5, the point $\delta(x) \in (k^*)^n$ is a zero of $\text{in}_w(f)$, and then, by the semiregularity of F at w , we have $\det \left(\frac{\partial \text{in}_w(f_i)}{\partial X_j} \right) \Big|_{\delta(x)} \neq 0$. Again by Lemma 2.5, this means that $\det \left(\pi^{w_j - \text{tr}(f_i)} \frac{\partial f_i}{\partial X_j} \Big|_x \right) \not\equiv 0 \pmod{\mathfrak{M}}$, and by factoring out the powers of π of the determinant, we conclude that $v(\text{Jac}(F)(x)) = \text{tr}(f_1; w) + \dots + \text{tr}(f_n; w) - (w_1 + \dots + w_n)$. \square

The following three lemmas show how semiregularity behaves with respect to a rescaling of variables and multiplication by monomials.

Lemma 3.5. *Let $F = (f_1, \dots, f_n)$ be a system of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $w \in \mathbb{R}^n$, $a_1, \dots, a_n \in K^*$, and $\alpha_1, \dots, \alpha_n \in \mathbb{Z}^n$. Then F is semiregular at w if and only if $\tilde{F} = (a_1 X^{\alpha_1} f_1, \dots, a_n X^{\alpha_n} f_n)$ is semiregular at w .*

Proof. By the item 2 of Lemma 2.6, we have that $\text{Trop}(F) = \text{Trop}(\tilde{F})$, and since the claim is symmetric, it is enough to prove that when $w \in \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$ and $\text{in}_w(F)$ has no degenerate zero in $(k^*)^n$ then also $\text{in}_w(\tilde{F})$ has no degenerate zero. By the item 4 of Lemma 2.6, we have that $\text{in}_w(\tilde{F}) = (\delta(a_1) X^{\alpha_1} \text{in}_w(f_1), \dots, \delta(a_n) X^{\alpha_n} \text{in}_w(f_n))$, and in particular, $\text{in}_w(F)$ and $\text{in}_w(\tilde{F})$ have the same zeros in (k^*) . Let $x \in (k^*)^n$ be one of these zeros, which by assumption is a non-degenerate zero of $\text{in}_w(F)$. We have to show that x is also a non-degenerate zero of $\text{in}_w(\tilde{F})$. The Jacobian of $\text{in}_w(\tilde{F})$ is given by the following expression.

$$\text{Jac}(\text{in}_w(\tilde{F})) = \det \left(\delta(a_i) \alpha_{ij} X^{\alpha_i - e_j} \text{in}_w(f_i) + \delta(a_i) X^{\alpha_i} \frac{\partial \text{in}_w(f_i)}{\partial X_j} \right)_{1 \leq i, j \leq n}$$

Evaluating at $X = x$ we get $\text{Jac}(\text{in}_w(\tilde{F}))(x) = \delta(a_1 \cdots a_n) x^{\alpha_1 + \cdots + \alpha_n} \text{Jac}(\text{in}_w(F))(x)$, which is not zero in k^* , since x is a non-degenerate zero of $\text{in}_w(F)$. \square

Lemma 3.6. *Let $F = (f_1, \dots, f_n)$ be a system of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $w \in \mathbb{R}^n$ and $b = (b_1, \dots, b_n) \in (K^*)^n$. Then F is semiregular at w if and only if the system with rescaled variables $\tilde{F} = (f_1(b_1 X_1, \dots, b_n X_n), \dots, f_n(b_1 X_1, \dots, b_n X_n))$ is semiregular at $w - v(b)$.*

Proof. By the item 6 of Lemma 2.6, we have that $\text{Trop}(\tilde{F}) = \text{Trop}(F) - v(b)$. Since $v(b) \in v(\pi)\mathbb{Z}^n$, then $w \in \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$ if and only if $w \in \text{Trop}(\tilde{F}) \cap v(\pi)\mathbb{Z}^n$. By the symmetry of the claim, it is enough to show that when $w \in \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$ and $\text{in}_w(F)$ has no degenerate zero in $(k^*)^n$, then also $\text{in}_{w-v(b)}(\tilde{F})$ has no degenerate zero. By the item 8 of Lemma 2.6, we have that $\text{in}_{w-v(b)}(\tilde{F}) = (\text{in}_w(f_1)(\delta(b)X), \dots, \text{in}_w(f_n)(\delta(b)X))$, and in particular, if $x \in (k^*)^n$ is a zero of $\text{in}_{w-v(b)}(\tilde{F})$, then $y = \delta(b)x$ is a zero of $\text{in}_w(F)$. A simple computation using the chain rule shows that $\text{Jac}(\text{in}_{w-v(b)}(\tilde{F}))(x) = \delta(b_1 \cdots b_n) \text{Jac}(\text{in}_w(F))(y)$. Since the right hand side does not vanish at any zero y of $\text{in}_w(F)$, then the zeros of $\text{in}_{w-v(b)}(\tilde{F})$ are all non-degenerate. \square

Lemma 3.7. *Let F be a system of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and let $w \in \text{Trop}(F)$. Then F is semiregular (resp. normalized) at w if and only if $F^{[w]}$ is semiregular (resp. normalized) at w .*

Proof. The claim that F is normalized at w if and only if $F^{[w]}$ is normalized at w follows from the fact that $\text{tr}(f_i; w) = \text{tr}(f_i^{[w]}; w)$ for all $i = 1, \dots, n$. The claim about semiregularity is immediate from $\text{in}_w(F) = \text{in}_w(F^{[w]})$. \square

At this point we have all the necessary ingredients for the main result of this section, which is a reformulation of Hensel's Lemma in the language of Definition 3.3. For pedagogical reasons, we start with the classical statement, and then, we reformulate it progressively until we arrive to the final version in Corollary 3.12.

Lemma 3.8 (Hensel). *Let F be a system of n polynomials in $A[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and denote by \overline{F} the system reduced modulo \mathfrak{M} . Let $\overline{x} \in (k^*)^n$ be a solution of \overline{F} such that $\text{Jac}(\overline{F})(\overline{x}) \neq 0$. Then there exists a unique solution $x \in (A \setminus \mathfrak{M})^n$ of F such that $\overline{x} = x \pmod{\mathfrak{M}}$.*

Proof. See [4, Prop. 2.11]. \square

Lemma 3.9. *Let F be a system of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ such that $0 \in \text{Trop}(F)$. Assume also that F is normalized and semiregular at 0. Then all the coefficients of F are in the valuation ring A . Moreover, the reduction map $\text{mod } \mathfrak{M} : A^n \rightarrow k^n$ induces a bijection between the set of zeros of F in $(K^*)^n$ with valuation vector 0 (i.e. in $(A \setminus \mathfrak{M})^n$) and the set of zeros of \overline{F} in $(k^*)^n$.*

Proof. Suppose that $F = (f_1, \dots, f_n)$. Since the system is normalized at 0, we have $\text{tr}(f_i; 0) = 0$ for all $i = 1, \dots, n$. Since $\text{tr}(f_i; 0)$ is the minimum valuation of the coefficients of f_i , then all the coefficients of f_i have valuation at least 0, i.e. $f_i \in A[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Moreover, the terms of f_i that are kept in $\text{in}_0(f_i)$ are those with coefficients in $A \setminus \mathfrak{M}$. For these terms, reducing modulo \mathfrak{M} or taking first digit is exactly the same, so $\overline{f_i} = \text{in}_0(f_i)$. In particular, we have that $\overline{F} = \text{in}_0(F)$ has no degenerate solutions in $(k^*)^n$. It is clear that the reduction modulo \mathfrak{M} maps zeros of F in $(K^*)^n$

with valuation 0 to zeros of \overline{F} in $(k^*)^n$. We only have to show that the map is a bijection. For the surjectivity, take a zero of \overline{F} in $(k^*)^n$. The semiregularity at 0 guarantees that it is non-degenerate zero, and Lemma 3.8 shows that it can be lifted to a zero of F in $(A \setminus \mathfrak{M})^n$, i.e. to a zero of F with valuation 0. The injectivity follows from the uniqueness of the lifting in Hensel's Lemma. \square

Definition 3.10. *For any system of polynomials F in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$, the set of roots of F in $(K^*)^n$ is denoted by $Z_K(F)$, and the set of zeros of F with valuation w is written $Z_K^w(F)$.*

Theorem 3.11. *Let F be a system of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $w \in \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n$ and suppose that F is semiregular at w . The first digit maps $\delta : Z_K^w(F) \rightarrow Z_k(\text{in}_w(F))$ and $\delta : Z_K^w(F^{[w]}) \rightarrow Z_k(\text{in}_w(F))$ are bijections (and are well-defined between these sets of roots).*

Proof. The case $w = 0$ and F normalized at 0 follows immediately from Lemmas 3.9 and 3.7 and the fact that the reductions of F and $F^{[0]}$ modulo \mathfrak{M} coincide with $\text{in}_0(F)$. Note that the assumption that F is normalized at 0 can be easily removed by pre-multiplying each equation in F by a suitable constant in K^* . We can also reduce the general case to $w = 0$ by a simple change of variables. Define $\hat{F} = F(\pi^{w_1/v(\pi)}X_1, \dots, \pi^{w_n/v(\pi)}X_n)$. By Lemma 3.6, the system \hat{F} is semiregular at 0. It is clear that the first digit preserving map $(x_1, \dots, x_n) \mapsto (\pi^{w_1/v(\pi)}x_1, \dots, \pi^{w_n/v(\pi)}x_n)$ is a bijection between the set of solutions of \hat{F} with valuation vector 0 and the zeros of F with valuation w . Moreover, by the item 8 of Lemma 2.6, we have $\text{in}_w(F) = \text{in}_0(\hat{F})$, and by the item 7 we have $F^{[w]}(\pi^{w_1/v(\pi)}X_1, \dots, \pi^{w_n/v(\pi)}X_n) = \hat{F}^{[0]}$. This provides the reduction to the case $w = 0$. \square

Although the previous result contains all the substance of this section, the following corollary is the way Theorem 3.11 is intended to be used in practice.

Corollary 3.12. *Let F be a system of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Assume that F is semiregular at w . Then there is a unique bijection between the sets $Z_K^w(F)$ and $Z_K^w(F^{[w]})$ that preserves first digits. If $w \notin \text{Trop}(F)$ or $w \notin v(\pi)\mathbb{Z}^n$, then these sets are empty. Otherwise, the first digit map gives bijections from $Z_K^w(F)$ and $Z_K^w(F^{[w]})$ to $Z_k(\text{in}_w(F))$.*

A more computational point of view is shown in the following algorithm.

Algorithm 1 Decide whether a system $F = (f_1, \dots, f_n)$ of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ is semiregular at a given point $w = (w_1, \dots, w_n) \in \mathbb{R}^n$. In case of semiregularity, print the number of solutions in $(K^*)^n$ with valuation vector w .

```

1: if  $w \notin v(\pi)\mathbb{Z}^n$  then
2:   print the system has no solutions in  $(K^*)^n$  with valuation  $w$ 
3:   return YES
4: end if
5: for  $i = 1, \dots, n$  do
6:    $\tilde{f}_i \leftarrow \text{in}_w(f_i)$ 
7:   if  $\tilde{f}_i$  is a monomial then
8:     print the system has no solutions in  $(K^*)^n$  with valuation  $w$ 
9:     return YES
10:  end if
11: end for
12:  $\text{Jac}(\tilde{F}) \leftarrow \det(\partial \tilde{f}_i / \partial X_j)$ 
13: if there is a solution of  $\tilde{f}_1(x) = \dots = \tilde{f}_n(x) = \text{Jac}(\tilde{F})(x) = 0$  in  $(k^*)^n$  then
14:   return NO
15: end if
16:  $s \leftarrow$  number of solutions of  $\tilde{f}_1(x) = \dots = \tilde{f}_n(x) = 0$  in  $(k^*)^n$ 
17: print the system has  $s$  solutions in  $(K^*)^n$  with valuation  $w$ 
18: return YES

```

In case that only an estimation for the number of zeros is needed, the following statement might be useful.

Corollary 3.13. *Let F be a system of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. If $\text{Trop}(F)$ is finite and F is semiregular at any $w \in \text{Trop}(F)$, then the number of solutions of F in $(K^*)^n$ is*

$$|Z_K(F)| = \sum_{w \in \text{Trop}(F) \cap v(\pi)\mathbb{Z}^n} |Z_k(\text{in}_w(F))| \leq |\text{Trop}(F) \cap v(\pi)\mathbb{Z}^n| \cdot |k^*|^n \leq |\text{Trop}(F)| \cdot |k^*|^n.$$

Note that when $\text{Trop}(F)$ is a finite set, then it has at most $\prod_{i=1}^n \binom{t_i}{2}$ points, where t_i is the number of monomials of f_i . Each $\text{Trop}(f_i)$ is contained in the union of $\binom{t_i}{2}$ hyperplanes (see Lemma 2.2), and the intersection of n of these hyperplanes (one in each $\text{Trop}(f_i)$) determines at most one point in $\text{Trop}(F)$. In particular, a system F that satisfies the hypothesis of Corollary 3.13 has at most $\binom{t_1}{2} \cdots \binom{t_n}{2} |k^*|^n$ roots in $(K^*)^n$, and all these roots are non-degenerate.

We conclude this section with a discussion of the univariate case. Consider $f = \sum_{i=1}^t a_i X^{\alpha_i} \in K[X]$. In section 2, we showed that the tropical hypersurface of f is the set of minus the slope of the segments of the lower hull of $\text{NP}(f)$. For each of these $w \in \text{Trop}(f)$, the lower polynomial $f^{[w]}$ and initial form $\text{in}_w(f)$ are simply the polynomials obtained by keeping only the terms with $(\alpha_i, v(a_i))$ lying on the segment of slope $-w$. For each $w \in \text{Trop}(f)$, semiregularity at w means that either $w \notin v(\pi)\mathbb{Z}$, in which case f has no solutions in K^* with valuation w , or $\text{in}_w(f)$ has no degenerate zeros in k^* . In case of semiregularity at $w \in \text{Trop}(f) \cap v(\pi)\mathbb{Z}$, our main result says that the number of roots of f in K^* with valuation w and the number of roots of $\text{in}_w(f)$ in k^* coincide.

4 Regularity.

Definition 4.1. A system F of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ is regular if $\text{Trop}(F)$ is finite, $F^{[w]}$ consists solely of binomials and F is semiregular at w for all $w \in \text{Trop}(F)$.

For this kind of system, we can provide an explicit formula for the number of roots in $(K^*)^n$. We will also give a different characterization of regularity that is easier to check. First of all, the notion of regularity is well-behaved under monomial changes of variables.

Lemma 4.2. Let $F = (f_1, \dots, f_n)$ be a system of polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $a_1, \dots, a_n \in K^*$, $b_1, \dots, b_n \in K^*$, and $\alpha_1, \dots, \alpha_n \in \mathbb{Z}^n$. The following three statements are equivalent.

1. F is regular.
2. $(a_1 X^{\alpha_1} f_1, \dots, a_n X^{\alpha_n} f_n)$ is regular.
3. $(f_1(b_1 X_1, \dots, b_n X_n), \dots, f_n(b_1 X_1, \dots, b_n X_n))$ is regular.

Proof. A consequence of Lemmas 2.6, 3.5 and 3.6. □

The problem of deciding whether a system is regular or not can be reduced to the case of binomial systems: in Definition 4.1, the condition F is semiregular at w can be replaced, according to Lemma 3.7, by the condition $F^{[w]}$ is semiregular at w . The following lemma and proposition characterize semiregularity for binomial systems.

Lemma 4.3. Consider a binomial system $B = (a_1 X^{\alpha_1} - b_1 X^{\beta_1}, \dots, a_n X^{\alpha_n} - b_n X^{\beta_n})$ with coefficients $a = (a_1, \dots, a_n) \in (K^*)^n$, let $b = (b_1, \dots, b_n) \in (K^*)^n$, and let $M \in \mathbb{Z}^{n \times n}$ be the matrix whose i -th row is $\alpha_i - \beta_i$ for $i = 1, \dots, n$. Then

$$\text{Trop}(B) = \{w \in \mathbb{R}^n : Mw = v(b) - v(a)\}.$$

In particular, $\text{Trop}(B)$ is finite (and non-empty) if and only if $\det(M) \neq 0$.

Proof. By Lemma 2.2, the tropical hypersurface of the i -th binomial is $\text{Trop}(a_i X^{\alpha_i} - b_i X^{\beta_i}) = \{w \in \mathbb{R}^n : v(a_i) + \alpha_i \cdot w = v(b_i) + \beta_i \cdot w\}$. This equation corresponds with the i -th row of $Mw = v(b) - v(a)$. □

For any vector $x = (x_1, \dots, x_n)$ with non-zero entries and any matrix $M = (m_{ij})_{1 \leq i, j \leq n} \in \mathbb{Z}^{n \times n}$, we write

$$x^M = (x_1^{m_{11}} \dots x_n^{m_{1n}}, \dots, x_1^{m_{n1}} \dots x_n^{m_{nn}}).$$

Note that if $P, Q \in \mathbb{Z}^{n \times n}$, then $x^{PQ} = (x^Q)^P$.

Proposition 4.4. Consider the binomial system $B = (a_1 X^{\alpha_1} - b_1 X^{\beta_1}, \dots, a_n X^{\alpha_n} - b_n X^{\beta_n})$ in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$. Let $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$. Assume that the matrix $M \in \mathbb{Z}^{n \times n}$, whose i -th row is $\alpha_i - \beta_i$ for $i = 1, \dots, n$, has non-zero determinant. Let $M = PDQ$ be the Smith Normal Form of M , i.e. $P, Q \in \mathbb{Z}^{n \times n}$ are invertible and $D = \text{diag}(d_1, \dots, d_n)$ with $d_1 \mid d_2 \mid \dots \mid d_n$ positive integers. Then B is semiregular at $w = M^{-1}(v(b) - v(a))$ if and only if either:

1. $w \notin v(\pi)\mathbb{Z}^n$.
2. $\text{char}(k) \nmid \det(M)$.
3. the i -th entry of $(\delta(b_1/a_1), \dots, \delta(b_n/a_n))^{P^{-1}}$ is not a d_i -th power in k^* for some $i = 1, \dots, n$.

In this case, if (1) and (3) do not hold, then the number of solutions of the system B in $(K^*)^n$ is $|Z_K(B)| = \prod_{i=1}^n |\{\xi \in k^* : \xi^{d_i} = 1\}|$. Otherwise B has no solutions in $(K^*)^n$.

Proof. By Lemma 4.2, we have $w \in \text{Trop}(B)$. In case that $w \notin v(\pi)\mathbb{Z}^n$, then B is semiregular at w by definition, B has no solutions in $(K^*)^n$ since there are no elements in $(K^*)^n$ with valuation w , and the proposition is proven. Now assume that $w \in v(\pi)\mathbb{Z}^n$. By Lemma 3.5, the system B is semiregular at w if and only if the system $X^M = b/a$ is semiregular at w . The initial form system is $X^M = \delta(b/a)$. Any solution $x \in (K^*)^n$ of this system satisfies $(x^Q)^D = (\delta(b/a))^{P^{-1}}$ and then the condition of item 3 is not met. In other words, if the system satisfies the third condition, then the initial form system (and also B) has no solution, B is automatically semiregular at w , and the proposition is proven. So we can assume without loss of generality that B does not satisfy items 1 and 3. In this case, there exist $y \in (k^*)^n$ such that $y^D = (\delta(b/a))^{P^{-1}}$, and then $x = y^{Q^{-1}} \in (k^*)^n$ is a zero of $X^M = \delta(b/a)$. The Jacobian of this system is $J = \det([m_{ij}X_1^{m_{i1}} \dots X_j^{m_{ij}-1} \dots X_n^{m_{in}}]_{1 \leq i, j \leq n})$, which, after factoring out X_j^{-1} from the j -th column, and then $X_1^{m_{i1}} \dots X_n^{m_{in}}$ from the i -th row, becomes a single term with coefficient $\det(M)$. In particular, a solution $x \in (k^*)^n$ of $X^M = \delta(b/a)$ is non-degenerate if and only if $\text{char}(k) \nmid \det(M)$. This shows the equivalence between semiregularity of B at w and item 2. Finally, the number of solutions of $X^M = \delta(b/a)$ is equal to the number of solutions of $Y^D = (\delta(b/a))^{P^{-1}}$, since the map $x \mapsto x^Q$ is a bijection. We know already that there is a solution $y \in (k^*)^n$, and it is clear that all other solution can be obtained by multiplying the i -th entry of y by a d_i -th root of unity in k^* . This proves the formula for the number of zeros of B . \square

A system of polynomials F is regular if and only if $\text{Trop}(F)$ is finite and $F^{[w]}$ is a binomial system that satisfies the assumptions of Proposition 4.4 for all $w \in \text{Trop}(F)$. In this case, an explicit formula for the number of roots of F in $(K^*)^n$ can be obtained from Corollary 3.13 and Proposition 4.4. The following algorithm summarizes this procedure.

Algorithm 2 Decides whether a system $F = (f_1, \dots, f_n)$ of n polynomials in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ is regular. In case of regularity, it prints the number of solutions in $(K^*)^n$.

```

1: compute  $\text{Trop}(F) \leftarrow \text{Trop}(f_1) \cap \dots \cap \text{Trop}(f_n)$ 
2: if  $|\text{Trop}(F)| = \infty$  then
3:   return NO
4: end if
5:  $s \leftarrow 0$ 
6: for all  $w \in \text{Trop}(F)$  do
7:   if  $f_1^{[w]}, \dots, f_n^{[w]}$  are not all binomials then
8:     return NO
9:   else
10:    write each  $f_i^{[w]}$  as  $a_i X^{\alpha_i} - b_i X^{\beta_i}$  for  $i = 1, \dots, n$ .
11:     $M \leftarrow [\alpha_1 - \beta_1; \dots; \alpha_n - \beta_n]$ 
12:    compute the Smith Normal Form  $PDQ$  of  $M$ 
13:     $\rho \leftarrow (\delta(b_1/a_1), \dots, \delta(b_n/a_n))^{P^{-1}}$ 
14:    if  $w \in v(\pi)\mathbb{Z}^n$  and  $\rho_i$  is a  $d_i$ -th power in  $k^*$  for all  $i = 1, \dots, n$  then
15:      if  $\text{char}(k) \mid d_1 \cdots d_n$  then
16:        return NO
17:      else
18:         $e_i \leftarrow |\{\xi \in k^* : \xi^{d_i} = 1\}|$  for  $i = 1, \dots, n$ 
19:         $s \leftarrow s + \prod_{i=1}^n e_i$ 
20:      end if
21:    end if
22:  end if
23: end for
24: print the system has  $s$  solutions in  $(K^*)^n$ 
25: return YES

```

Algorithm 2 is presented above in pseudo-code with the maximum generality, in order to match the notation and logic behind Proposition 4.4. In any real implementation of the algorithm, the test in line 15 and the formula in line 19, should be replaced by some specific instructions depending on the field k .

- When k is a finite field of cardinality $q = |k|$, the test in line 15 can be rewritten as $\rho_i^{(q-1)/\gcd(q-1, d_i)} = 1$, and line 19 can be replaced by $e_i \leftarrow \gcd(q-1, d_i)$.
- When k is algebraically closed, line 15 can be simply skipped, since this tests always yields true, and line 19 becomes $e_i \leftarrow d_i$, or more simply, line 20 becomes $s \leftarrow s + |\det(M)|$ and line 19 is deleted.
- When $\text{char}(k) = 0$, the test made in line 16 is not necessary, since by Lemma 4.3, the matrix M in line 11 has non-zero determinant, and therefore $d_1 \cdots d_n = \det(D) = |\det(M)| \neq 0$.

In the univariate case, regular polynomials are very easy to describe. First of all, the tropical hypersurface of a univariate polynomial is always finite. Moreover, for each w in the tropical set,

the lower polynomial $f^{[w]}$ contains all the monomials aX^α of f such that the point $(\alpha, v(a))$ lies on the lower edge of $\text{NP}(f)$ with slope w . This means that, in order to have regularity, the lower edges of $\text{NP}(f)$ must not contain any point (corresponding to a monomial of f) other than the vertices. In addition to this, each lower binomial $f^{[w]} = aX^\alpha + bX^\beta$ must have either $w \notin v(\pi)\mathbb{Z}$, or $\text{char}(k) \nmid \alpha - \beta$, or $\delta(b/a)$ not a $(\alpha - \beta)$ -th power in k^* . Compared with the notion of regularity given in [2, Def. 1], the definition in this paper includes a broader class of polynomials, while the formula for the total number of roots in K^* provided in [2, Thm. 4.4, Thm. 4.5] is the same as the formula implied by our Algorithm 2.

Consider a set $\mathcal{A} = \{\alpha_1 < \dots < \alpha_t\} \subseteq \mathbb{Z}$ with $t \geq 2$. Denote $K[X]_{\mathcal{A}}$ the set of polynomial supported by \mathcal{A} , i.e. $K[X]_{\mathcal{A}} = \{\sum_{\alpha \in \mathcal{A}} a_\alpha X^\alpha : a_\alpha \neq 0\}$. For each $f \in K[X]_{\mathcal{A}}$ we define the support of the Newton Polygon of f as the set $\mathcal{B} = \{\alpha \in \mathcal{A} : (\alpha, v(a_\alpha)) \in \text{lower hull of } \text{NP}(f)\}$. The subset of the polynomials in $K[X]_{\mathcal{A}}$ with Newton Polygon supported at \mathcal{B} is denoted $K[X]_{\mathcal{A}}^{\mathcal{B}}$. Note that we always have $\{\alpha_1, \alpha_t\} \subseteq \mathcal{B} \subseteq \mathcal{A}$, and that $K[X]_{\mathcal{A}} = \bigcup_{\{\alpha_1, \alpha_t\} \subseteq \mathcal{B} \subseteq \mathcal{A}} K[X]_{\mathcal{A}}^{\mathcal{B}}$. The discussion above is summarized in the following corollary.

Corollary 4.5. *Let $\mathcal{A} = \{\alpha_1 < \dots < \alpha_t\} \subseteq \mathbb{Z}$ be a set with $t \geq 2$ and $\text{char}(k) \nmid \alpha_j - \alpha_i$ for all $i \neq j$. Let $\mathcal{B} = \{\alpha_1 = \beta_1 < \dots < \beta_{|\mathcal{B}|} = \alpha_t\} \subseteq \mathcal{A}$ and take $f = \sum_{\alpha \in \mathcal{A}} a_\alpha X^\alpha \in K[X]_{\mathcal{A}}^{\mathcal{B}}$. Then*

$$\text{Trop}(f) = \left\{ -\frac{v(a_{\beta_{i+1}}) - v(a_{\beta_i})}{\beta_{i+1} - \beta_i} : i = 1, \dots, |\mathcal{B}| - 1 \right\},$$

i.e. $\text{Trop}(f)$ is the set of minus the slopes of the segments of $\text{NP}(f)$. Moreover, f is regular if and only if the points $\{(\beta, v(a_\beta)) : \beta \in \mathcal{B}\}$ are all vertices of the Newton Polygon, and in this case, the number of roots of f in K^* is equal to

$$\sum_{i=1}^{|\mathcal{B}|-1} \chi_{v(\pi)\mathbb{Z}} \left(\frac{v(a_{\beta_{i+1}}) - v(a_{\beta_i})}{\beta_{i+1} - \beta_i} \right) \left| Z_k(\delta(a_{\beta_{i+1}})X^{\beta_{i+1}} + \delta(a_{\beta_i})X^{\beta_i}) \right|.$$

Finally, note that given a polynomial $f \in K[X]_{\mathcal{A}}$ and a subset $\{\alpha_1, \alpha_t\} \subseteq \mathcal{B} \subseteq \mathcal{A}$, it is possible to determine whether f belongs to $K[X]_{\mathcal{A}}^{\mathcal{B}}$ by just testing a few linear inequalities in the valuations of the coefficients: a point $\alpha \in \mathcal{A}$ is in the support of the Newton Polygon if and only if

$$v(a_\alpha) \leq v(a_{\alpha'}) \frac{\alpha - \alpha''}{\alpha' - \alpha''} + v(a_{\alpha''}) \frac{\alpha' - \alpha}{\alpha' - \alpha''}$$

for all $\alpha', \alpha'' \in \mathcal{A}$ with $\alpha' < \alpha < \alpha''$. Inspired by this simple test, we introduce the set $S(\mathcal{B}/\mathcal{A}) \subseteq \mathbb{R}^t$ defined as the set of all vectors $(v_1, \dots, v_t) \in \mathbb{R}^t$ such that

$$v_i \leq v_j \frac{\alpha_i - \alpha_k}{\alpha_j - \alpha_k} + v_k \frac{\alpha_j - \alpha_i}{\alpha_j - \alpha_k}$$

for all $1 \leq j < i < k \leq t$ if and only if $\alpha_i \in \mathcal{B}$. This means that a polynomial $f \in K[X]_{\mathcal{A}}$ belongs to $K[X]_{\mathcal{A}}^{\mathcal{B}}$ if and only if $(v(a_{\alpha_1}), \dots, v(a_{\alpha_t})) \in S(\mathcal{B}/\mathcal{A})$. In the analysis of random univariate polynomials of Section 6, we will need the Lebesgue measure of the set $S(\mathcal{B}/\mathcal{A}) \cap [0, 1]^t$, which will be denoted $P(\mathcal{B}/\mathcal{A})$. Roughly speaking, $P(\mathcal{B}/\mathcal{A})$ is the probability that the set of points $\{(\alpha_1, v_1), \dots, (\alpha_t, v_t)\}$, where $v_i \sim \mathcal{U}[0, 1]$ are independent random variables, has Newton Polygon supported at \mathcal{B} . From the form of the equations defining these sets, note that $(v_1, \dots, v_t) \in S(\mathcal{B}/\mathcal{A})$ if and only if $(av_1 + b, \dots, av_t + b) \in S(\mathcal{B}/\mathcal{A})$ for all $a, b \in \mathbb{R}$, i.e. these sets are invariant under rescaling and translations. In particular, the measure of $S(\mathcal{B}/\mathcal{A}) \cap [a, b]^t$ is equal to $(b - a)^t P(\mathcal{B}/\mathcal{A})$.

5 Tropical genericity of regular systems

Definition 5.1. Consider a proposition $P : (K^*)^n \rightarrow \{\text{True}, \text{False}\}$. We say that P is true for any generic $x \in (K^*)^n$ if and only if $P^{-1}(\text{False})$ is contained in an algebraic hypersurface of $(K^*)^n$. Similarly, a proposition $P : (K^*)^n \rightarrow \{\text{True}, \text{False}\}$ is said to be true for any tropically generic $x \in (K^*)^n$ if and only if $v(P^{-1}(\text{False}))$ is contained in a finite union of hyperplanes of \mathbb{R}^n .

Note that genericity implies tropical genericity: if a statement P is true for generic $x \in (K^*)^n$, then there is a hypersurface $Z_K(G) \subseteq (K^*)^n$ that contains $P^{-1}(\text{False})$, and therefore, the tropical hypersurface $\text{Trop}(G)$, which is contained in a finite union of hyperplanes of \mathbb{R}^n , contains $v(P^{-1}(\text{False}))$.

Let $\mathcal{A}_1, \dots, \mathcal{A}_n \subseteq \mathbb{Z}^n$ be nonempty finite sets. Consider a system of polynomials $F = (f_1, \dots, f_n)$ in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ with undetermined (non-zero) coefficients and $\text{Supp}(f_i) = \mathcal{A}_i$ for all $i = 1, \dots, n$. Let $N = |\mathcal{A}_1| + \dots + |\mathcal{A}_n|$ be the number of coefficients in F . Once these supports have been fixed, we can speak about propositions for generic or tropically generic systems F in the sense of Definition 5.1: the domain of the propositions is understood to be the coefficient space $(K^*)^N$ of the systems.

Theorem 5.2. Any tropically generic system $F = (f_1, \dots, f_n)$ in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ has finite tropical prevariety $\text{Trop}(F)$ and its lower polynomials $f_i^{[w]}$ are binomials for all $w \in \text{Trop}(F)$ and $i = 1, \dots, n$.

Proof. Write $f_i = \sum_{\alpha \in \mathcal{A}_i} a_{\alpha}^{(i)} X^{\alpha}$ for $i = 1, \dots, n$. Assume first that $\text{Trop}(F)$ is an infinite set. We will show that the vector $\mu = v(a_{\alpha}^{(i)})_{1 \leq i \leq n, \alpha \in \mathcal{A}_i} \in \mathbb{R}^N$ lies on a finite union of hyperplanes $H \subseteq \mathbb{R}^N$ that depends only on the sets $\mathcal{A}_1, \dots, \mathcal{A}_n$. By Lemma 3.5, there are $\alpha_i, \beta_i \in \mathcal{A}_i$ for $i = 1, \dots, n$ such that the system of linear equations

$$\begin{aligned} v(a_{\alpha_1}^{(1)}) + \alpha_1 \cdot w &= v(a_{\beta_1}^{(1)}) + \beta_1 \cdot w \\ \vdots & \\ v(a_{\alpha_n}^{(n)}) + \alpha_n \cdot w &= v(a_{\beta_n}^{(n)}) + \beta_n \cdot w \end{aligned} \tag{2}$$

has infinitely many solutions $w \in \mathbb{R}^n$. This means that the determinant of the matrix whose rows are $\alpha_i - \beta_i$ for $i = 1, \dots, n$ is zero and that

$$\left(v(a_{\alpha_1}^{(1)}) - v(a_{\beta_1}^{(1)}), \dots, v(a_{\alpha_n}^{(n)}) - v(a_{\beta_n}^{(n)}) \right) \in \langle \alpha_i - \beta_i : i = 1, \dots, n \rangle$$

Since the vectors $\alpha_i - \beta_i$ for $i = 1, \dots, n$ are \mathbb{R} -linearly dependent (the determinant of the matrix is zero), the subspace at the right side of the condition above has codimension one (or more) in \mathbb{R}^n . This translates into a condition that says that μ belongs to some hyperplane of \mathbb{R}^N that depends only on $\alpha_1, \beta_1, \dots, \alpha_n, \beta_n$. We conclude by taking H as the union of these hyperplanes for all possible choice of $\alpha_1, \beta_1 \in \mathcal{A}_1, \dots, \alpha_n, \beta_n \in \mathcal{A}_n$ such that $\{\alpha_i - \beta_i : i = 1, \dots, n\}$ is a \mathbb{R} -linearly dependent set.

Now assume that $\mu \notin H$, and in particular $\text{Trop}(F)$ is finite, but $f_i^{[w]}$ has three or more terms for some $i = 1, \dots, n$ and $w \in \text{Trop}(F)$. We will show that there is a finite union of hyperplanes

$H' \subseteq \mathbb{R}^N$, that depends only on $\mathcal{A}_1, \dots, \mathcal{A}_n$, such that $\mu \in H'$. It is enough to consider the case where the polynomial with three or more monomials is $f_1^{[w]}$. The point w is the unique solution of the system (2) for some $\alpha_1, \beta_1 \in \mathcal{A}_1, \dots, \alpha_n, \beta_n \in \mathcal{A}_n$, and in particular, the monomials $a_{\alpha_1}^{(1)} X^{\alpha_1}$ and $a_{\beta_1}^{(1)} X^{\beta_1}$ are in $f_1^{[w]}$. Since $f_1^{[w]}$ has three or more terms, there exists $\gamma_1 \in \mathcal{A}_1 \setminus \{\alpha_1, \beta_1\}$ such that the term $a_{\gamma_1}^{(1)} X^{\gamma_1}$ is in $f_1^{[w]}$. The equation $v(a_{\gamma_1}^{(1)}) + \gamma_1 \cdot w = v(a_{\alpha_1}^{(1)}) + \alpha_1 \cdot w$, where w is the unique solution of (2) expressed as a linear function of $v(a_{\alpha_1}^{(1)}), v(a_{\beta_1}^{(1)}), \dots, v(a_{\alpha_n}^{(n)}), v(a_{\beta_n}^{(n)})$ gives a non-trivial linear equation for the valuation of the coefficients of F , thus restricting μ to a hyperplane (that depends only on the choice of $\alpha_1, \beta_1, \gamma_1, \dots, \alpha_n, \beta_n$). We conclude by taking the union of all these possible hyperplanes. \square

According to Algorithm 2, a system F can fail to be regular for three different reasons (see lines 3, 8 and 17): when the tropical prevariety is not finite, when some lower polynomial has more than two terms, or when $\text{char}(k)$ divides the determinant of certain invertible matrices. By Theorem 5.2, the first two do not occur for tropically generic systems, and in particular, if $\text{char}(k) = 0$, then any tropically generic system is regular. The same idea works for any characteristic coprime to all the determinants that can arise in the test in line 16.

Corollary 5.3. *Let $\mathcal{A}_1, \dots, \mathcal{A}_n \subseteq \mathbb{Z}^n$ be nonempty finite sets. Assume that $\text{char}(k) = 0$ or that $\text{char}(k)$ is coprime to the determinant of all invertible matrices $M = [\alpha_1 - \beta_1; \dots; \alpha_n - \beta_n]$ with $\alpha_i, \beta_i \in \mathcal{A}_i$ for $i = 1, \dots, n$. Then, any tropically generic system of polynomials $F = (f_1, \dots, f_n)$ in $K[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ with $\text{supp}(f_i) = \mathcal{A}_i$ for $i = 1, \dots, n$ is regular.*

6 The expected number of roots of a random polynomial

In this section we restrict the discussion to univariate polynomials. Let $\mathcal{A} \subseteq \mathbb{Z}$ be a nonempty finite set. Assume that the characteristic of the residue field is either zero or coprime to $\alpha - \beta$ for all $\alpha, \beta \in \mathcal{A}$ with $\alpha \neq \beta$. This assumption ensures, by Corollary 5.3, that any tropically generic polynomial $f \in K[X]$ with support \mathcal{A} is regular. Since we have an explicit formula for the number of roots of regular polynomials in K^* , we should be able to obtain the expected number of roots of f in K^* , provided that we select the coefficients of f at random with a distribution that produces tropically generic polynomials with probability 1.

Let D_1 be a probability distribution on k^* , let D_2 be a probability distribution on $1 + \mathfrak{M}$, and let $M > 0$. We will select elements in K^* at random by selecting their valuation uniformly in $[-M, M] \cap v(\pi)\mathbb{Z}$, their first digit according to D_1 , and their tail in $1 + \mathfrak{M}$ according to D_2 . This procedure induces a probability distribution in K^* that extends to a distribution in $K[X]_{\mathcal{A}} = \{f \in K[X] : \text{supp}(f) = \mathcal{A}\}$. Denote by $E(\mathcal{A}, D_1, D_2, M, K)$ the expected number of roots in K^* of a polynomial $f \in K[X]_{\mathcal{A}}$ chosen at random with this distribution. Since the number of roots of these polynomials can not exceed their degree, we have that $E(\mathcal{A}, D_1, D_2, M, K) \leq \max_{\alpha, \beta \in \mathcal{A}} |\alpha - \beta|$. The main goal of this section is to find the value of

$$E(\mathcal{A}, D_1, D_2, K) = \lim_{M \rightarrow \infty} E(\mathcal{A}, D_1, D_2, M, K)$$

for several fields K and probability distributions D_1 and D_2 .

Lemma 6.1. *Consider the probability distribution in $K[X]_{\mathcal{A}}$ induced by D_1 , D_2 , and $M > 0$. Assume that $\text{char}(k)$ is zero or coprime to $\alpha - \beta$ for all $\alpha, \beta \in \mathcal{A}$ with $\alpha \neq \beta$. Then, the probability that a random $f \in K[X]_{\mathcal{A}}$ is not regular approaches zero as $M \rightarrow \infty$.*

Proof. Let $t = |\mathcal{A}|$ and $\mathcal{A} = \{\alpha_1, \dots, \alpha_t\}$. By Corollary 5.3, there are hyperplanes $H_1, \dots, H_n \subseteq \mathbb{R}^t$ such that any polynomial $f = \sum_{i=1}^t a_i X^{\alpha_i}$ with $(v(a_1), \dots, v(a_t)) \notin \cup_{j=1}^n H_j$ is regular. In particular, it is enough to show that the probability that a random $f \in K[X]_{\mathcal{A}}$ has coefficients with valuation in $\cup_{j=1}^n H_j$ goes to zero as $M \rightarrow \infty$. Note that this probability does not depend on the distributions D_1 and D_2 . Moreover, since the valuation of the coefficients is selected at random in the box $([-M, M] \cap v(\pi)\mathbb{Z})^t$ with uniform distribution, the probability of being in the union of n hyperplanes is less than or equal to $n/(2[M/v(\pi)] + 1)$ (each hyperplane contains at most $1/(2[M/v(\pi)] + 1)$ of the points in the box). As the size of the box increases, this probability approaches zero. \square

By Lemma 6.1, the probability that a random $f \in K[X]_{\mathcal{A}}$ is regular approaches 1 as M goes to infinity. Besides, we have shown in Proposition 4.4 (or in Algorithm 2) that the number of solutions of a regular system does not depend on the tail of the coefficients. In particular, the value of $E(\mathcal{A}, D_1, D_2, K)$ does not depend on D_2 , and for this reason, it will be simply written as $E(\mathcal{A}, D_1, K)$.

Before stating the main result, we need to fix some notation. For any $\gamma \in \mathbb{N}$, we denote by $E_k(\gamma, D_1)$ the expected number of roots in k^* of the binomial $aX^\gamma + b$ with coefficients $a, b \in k^*$ chosen at random (independently) according to the distribution D_1 . For instance, when k is algebraically closed, we have $E_k(\gamma, D_1) = \gamma$ regardless of the distribution D_1 . If k is a finite field and D_1 is the uniform distribution in k^* , then $E_k(\gamma, D_1) = 1$, since the number of roots of $X^\gamma = -b/a$ is either zero or $\gcd(|k^*|, \gamma)$, and the latter happens only when $-b/a$ is a γ -th power in k^* which occurs with probability $1/\gcd(|k^*|, \gamma)$. A similar situation arises in the case $k = \mathbb{R}$ and D_1 a distribution such that $\mathbb{R}_{>0}$ and $\mathbb{R}_{<0}$ have each probability $1/2$: if γ is odd, then $X^\gamma = -b/a$ has always one real root, and if γ is even, the number of roots is either 0 or 2 depending on whether $\text{sgn}(ab)$ is 1 or -1 , but in both cases we have $E_k(\gamma, D_1) = 1$.

k	D_1	$E_k(\gamma, D_1)$
k alg. closed	any	γ
$k = \mathbb{R}$	$\text{Prob}(\mathbb{R}_{<0}) = \text{Prob}(\mathbb{R}_{>0}) = 1/2$	1
$ k < +\infty$	uniform in k^*	1

Theorem 6.2. *Let $\mathcal{A} = \{\alpha_1 < \alpha_2 < \dots < \alpha_t\} \subseteq \mathbb{Z}$ finite with $t \geq 2$. Assume that $\text{char}(k) = 0$ or that $\text{char}(k)$ is coprime to $\alpha - \beta$ for any pair of elements $\alpha, \beta \in \mathcal{A}$ with $\alpha \neq \beta$. Let D_1 be a probability distribution in k^* . Then*

$$E(\mathcal{A}, D_1, K) = \sum_{\{\alpha_1, \alpha_t\} \subseteq \mathcal{B} \subseteq \mathcal{A}} P(\mathcal{B}/\mathcal{A}) \sum_{i=1}^{|\mathcal{B}|-1} \frac{E_k(\beta_{i+1} - \beta_i, D_1)}{\beta_{i+1} - \beta_i}$$

where $\mathcal{B} = \{\alpha_1 = \beta_1 < \beta_2 < \dots < \beta_{|\mathcal{B}|} = \alpha_t\}$.

Proof. Let D_2 be any probability distribution in $1 + \mathfrak{M}$ and let $M > 0$. Random polynomials $f = \sum_{\alpha \in \mathcal{A}} a_\alpha X^\alpha \in K[X]_{\mathcal{A}}$ will be chosen according to D_1 , D_2 and M . For each subset $\mathcal{B} = \{\alpha_1 = \beta_1 < \dots < \beta_{|\mathcal{B}|} = \alpha_t\} \subseteq \mathcal{A}$, denote by $K[X]_{\mathcal{A}}^{\mathcal{B}}$ the set of polynomials $f \in K[X]_{\mathcal{A}}$ with Newton Polygon supported at \mathcal{B} . By definition, we have that

$$E(\mathcal{A}, D_1, D_2, M, K) = \int_{K[X]_{\mathcal{A}}} |Z_K(f)| df = \sum_{\substack{\{\alpha_1, \alpha_t\} \subseteq \mathcal{B} \\ \mathcal{B} \subseteq \mathcal{A}}} \int_{K[X]_{\mathcal{A}}^{\mathcal{B}}} |Z_K(f)| df$$

and also

$$E(\mathcal{A}, D_1, D_2, K) = \sum_{\substack{\{\alpha_1, \alpha_t\} \subseteq \mathcal{B} \\ \mathcal{B} \subseteq \mathcal{A}}} \lim_{M \rightarrow \infty} \int_{K[X]_{\mathcal{A}}^{\mathcal{B}}} |Z_K(f)| df.$$

For any $f \in K[X]_{\mathcal{A}}^{\mathcal{B}}$, define

$$N(f) = \sum_{i=1}^{|\mathcal{B}|-1} \chi_{v(\pi)\mathbb{Z}} \left(\frac{v(a_{\beta_{i+1}}) - v(a_{\beta_i})}{\beta_{i+1} - \beta_i} \right) \left| Z_k(\delta(a_{\beta_{i+1}})X^{\beta_{i+1}} + \delta(a_{\beta_i})X^{\beta_i}) \right|,$$

where $\chi_S(\cdot)$ represents the characteristic function of the set S . This gives a function $N : K[X]_{\mathcal{A}} \rightarrow \mathbb{N}_0$ that, by Proposition 4.4, coincides with $|Z_K(f)|$ for any $f \in K[X]_{\mathcal{A}}$ regular. Moreover, the difference $N(f) - |Z_K(f)|$ is bounded on $K[X]_{\mathcal{A}}$. By Theorem 5.2, the probability of the set of non-regular polynomials approaches 0 as M goes to infinity, and then we can also write

$$\begin{aligned} E(\mathcal{A}, D_1, D_2, K) &= \sum_{\substack{\{\alpha_1, \alpha_t\} \subseteq \mathcal{B} \\ \mathcal{B} \subseteq \mathcal{A}}} \lim_{M \rightarrow \infty} \int_{K[X]_{\mathcal{A}}^{\mathcal{B}}} N(f) df = \\ &= \sum_{\substack{\{\alpha_1, \alpha_t\} \subseteq \mathcal{B} \\ \mathcal{B} \subseteq \mathcal{A}}} \lim_{M \rightarrow \infty} \int_{K[X]_{\mathcal{A}}} \chi_{K[X]_{\mathcal{A}}^{\mathcal{B}}}(f) N(f) df = \\ &= \sum_{\substack{\{\alpha_1, \alpha_t\} \subseteq \mathcal{B} \\ \mathcal{B} \subseteq \mathcal{A}}} \sum_{i=1}^{|\mathcal{B}|-1} \lim_{M \rightarrow \infty} \int_{K[X]_{\mathcal{A}}} N_{\mathcal{B},i}(f) df \end{aligned}$$

where $N_{\mathcal{B},i}(f)$ is the expression

$$\chi_{K[X]_{\mathcal{A}}^{\mathcal{B}}}(f) \chi_{v(\pi)\mathbb{Z}} \left(\frac{v(a_{\beta_{i+1}}) - v(a_{\beta_i})}{\beta_{i+1} - \beta_i} \right) \left| Z_k(\delta(a_{\beta_{i+1}})X^{\beta_{i+1}} + \delta(a_{\beta_i})X^{\beta_i}) \right|.$$

Any polynomial $f \in K[X]_{\mathcal{A}}$ correspond with a unique point $(w, \delta, e) \in ([-M, M] \cap v(\pi)\mathbb{Z})^t \times (k^*)^t \times (1 + \mathfrak{M})^t$. Using this representation, we can write $\int_{K[X]_{\mathcal{A}}} N_{\mathcal{B},i}(f) df$ as the triple integral

$$\iiint \chi_{K[X]_{\mathcal{A}}^{\mathcal{B}}}(f) \chi_{v(\pi)\mathbb{Z}} \left(\frac{w_{\beta_{i+1}} - w_{\beta_i}}{\beta_{i+1} - \beta_i} \right) \left| Z_k(\delta_{\beta_{i+1}}X^{\beta_{i+1}} + \delta_{\beta_i}X^{\beta_i}) \right| de d\delta dw.$$

Since the function $\chi_{K[X]_{\mathcal{A}}^{\mathcal{B}}}(f) \chi_{v(\pi)\mathbb{Z}}((w_{\beta_{i+1}} - w_{\beta_i})/(\beta_{i+1} - \beta_i))$ depends only on w , and the function $|Z_k(\delta_{\beta_{i+1}}X^{\beta_{i+1}} + \delta_{\beta_i}X^{\beta_i})|$ depends only on δ , the triple integral above can be splitted as a product

of three simple integrals. More precisely, we have that $\int_{K[X]_{\mathcal{A}}} N_{\mathcal{B},i}(f) df = I_w I_{\delta} I_e$, where

$$\begin{aligned} I_w &= \int_{([-M,M] \cap v(\pi)\mathbb{Z})^t} \chi_{K[X]_{\mathcal{A}}}^{\mathcal{B}}(f) \chi_{v(\pi)\mathbb{Z}} \left(\frac{w_{\beta_{i+1}} - w_{\beta_i}}{\beta_{i+1} - \beta_i} \right) dw, \\ I_{\delta} &= \int_{(k^*)^t} \left| Z_k(\delta_{\beta_{i+1}} X^{\beta_{i+1}} + \delta_{\beta_i} X^{\beta_i}) \right| d\delta, \\ I_e &= \int_{(1+\mathfrak{M})^t} 1 de. \end{aligned}$$

It is clear that $I_e = 1$ and also $I_{\delta} = E_k(\beta_{i+1} - \beta_i, D_1)$ by definition. The integral defining I_w is in fact a finite sum over a lattice: if we write $N = \lfloor M/v(\pi) \rfloor$ and $v_{\alpha} = w_{\alpha}/v(\pi)$, then

$$\begin{aligned} I_w &= (2N+1)^{-t} \sum_{-N \leq v_1, \dots, v_t \leq N} \chi_{K[X]_{\mathcal{A}}}^{\mathcal{B}}(f) \chi_{\mathbb{Z}} \left(\frac{v_{\beta_{i+1}} - v_{\beta_i}}{\beta_{i+1} - \beta_i} \right) = \\ &= (2N+1)^{-t} \sum_{\substack{-N \leq v_1, \dots, v_t \leq N \\ \beta_{i+1} - \beta_i | v_{\beta_{i+1}} - v_{\beta_i}}} \chi_{K[X]_{\mathcal{A}}}^{\mathcal{B}}(f). \end{aligned}$$

The expression $\chi_{K[X]_{\mathcal{A}}}^{\mathcal{B}}(f)$ in the last sum is a function of $v_{\alpha_1}, \dots, v_{\alpha_t}$ that test whether the Newton Polygon of the set of points $\{(v_{\alpha}, \alpha) : \alpha \in \mathcal{A}\}$ is supported at \mathcal{B} , i.e. is equal to $\chi_{S(\mathcal{B}/\mathcal{A})}(v_{\alpha_1}, \dots, v_{\alpha_t})$. Since the set $S(\mathcal{B}/\mathcal{A})$ is invariant under rescaling and translations, then

$$I_w = (2N+1)^{-t} \sum_{\substack{-N \leq v_1, \dots, v_t \leq N \\ \beta_{i+1} - \beta_i | v_{\beta_{i+1}} - v_{\beta_i}}} \chi_{S(\mathcal{B}/\mathcal{A})} \left(\frac{N + v_{\alpha_1}}{2N+1}, \dots, \frac{N + v_{\alpha_t}}{2N+1} \right).$$

Without the condition $\beta_{i+1} - \beta_i | v_{\beta_{i+1}} - v_{\beta_i}$, the expression is exactly a Riemman sum of $\chi_{S(\mathcal{B}/\mathcal{A})}$, with a partition of $[0, 1]^t$ corresponding to the lattice $\{0, 1/(2N+1), \dots, 1\}^t$. Adding this extra condition is equivalent to taking a sublattice of order $\beta_{i+1} - \beta_i$, so $\lim_{M \rightarrow \infty} I_w = P(\mathcal{B}/\mathcal{A})(\beta_{i+1} - \beta_i)^{-1}$. This shows that

$$\lim_{M \rightarrow \infty} \int_{K[X]_{\mathcal{A}}} N_{\mathcal{B},i}(f) df = P(\mathcal{B}/\mathcal{A}) \frac{E_k(\beta_{i+1} - \beta_i, D_1)}{\beta_{i+1} - \beta_i}.$$

Going back to our formula for $E(\mathcal{A}, D_1, D_2, K)$, we get

$$E(\mathcal{A}, D_1, D_2, K) = \sum_{\{\alpha_1, \alpha_{|\mathcal{A}|}\} \subseteq \mathcal{B} \subseteq \mathcal{A}} P(\mathcal{B}/\mathcal{A}) \sum_{i=1}^{|\mathcal{B}|-1} \frac{E_k(\beta_{i+1} - \beta_i, D_1)}{\beta_{i+1} - \beta_i}.$$

To conclude the proof, note that the right term does not depend on the probability distribution D_2 , and then we can safely write $E(\mathcal{A}, D_1, K)$, as claimed. \square

We conclude this section with an analysis of the case where the residue field is algebraically closed. In this case, we have $E_k(\gamma, D_1) = \gamma$, regardless of the probability distribution D_1 , so the formula of Theorem 6.2 reduces to

$$E(\mathcal{A}, D_1, K) = \sum_{\{\alpha_1, \alpha_{|\mathcal{A}|}\} \subseteq \mathcal{B} \subseteq \mathcal{A}} P(\mathcal{B}/\mathcal{A})(|\mathcal{B}| - 1) = 1 + \sum_{i=2}^t P_i,$$

where $P_i = \sum_{\{\alpha_1, \alpha_i, \alpha_{|\mathcal{A}|}\} \subseteq \mathcal{B} \subseteq \mathcal{A}} P(\mathcal{B}/\mathcal{A})$ is the probability that α_i is in the support of the Newton Polygon. The value of P_i can be written in terms of integrals, as shown in the following formula:

$$P_i = \int_0^1 \cdots \int_0^1 \min_{1 \leq j < i < k \leq t} \left(v_j \frac{\alpha_i - \alpha_k}{\alpha_j - \alpha_k} + v_k \frac{\alpha_j - \alpha_i}{\alpha_j - \alpha_k} \right) dv_1 \cdots \widehat{dv_i} \cdots dv_t.$$

The estimations

$$P_i \leq \int_0^1 \cdots \int_0^1 \max(\min(v_1, \dots, v_{i-1}), \min(v_{i+1}, \dots, v_t)) dv_1 \cdots \widehat{dv_i} \cdots dv_t,$$

$$P_i \geq \int_0^1 \cdots \int_0^1 \min(v_1, \dots, \widehat{v_i}, \dots, v_t) dv_1 \cdots \widehat{dv_i} \cdots dv_t,$$

show that $\frac{1}{t} \leq P_i \leq \frac{1}{i} + \frac{1}{t-i+1} - \frac{1}{t}$, and therefore

$$2 - \frac{2}{t} \leq E(\mathcal{A}, D_1, K) \leq 2 \sum_{i=2}^t \frac{1}{i} \leq 2 \ln(t).$$

Acknowledgements

We would like to thank Maurice Rojas and Bernd Sturmfels for several fruitful discussions about regularity and semiregularity, and for encouraging us to publish these results.

References

- [1] M. Avendaño: *Descartes' rule is exact!* Journal of Algebra, vol. 324(10), pp. 2884–2892, 2010.
- [2] M. Avendaño, A. Ibrahim: *Ultrametric root counting*. Houston Journal of Mathematics, vol. 36(4), pp. 1011–1022, 2010.
- [3] M. Avendaño, T. Krick: *Sharp bounds for the number fo roots of univariate fewnomials*. Journal of Number Theory, vol. 131(7), pp. 1209–1228, 2011.
- [4] M. Avendaño, T. Krick, A. Pacetti: *Newton-Hensel interpolation lifting*. Foundations of Computational Mathematics, vol. 6(1), pp. 81–120, 2006.
- [5] D. Bernstein: *The number of roots of a system of equations*. Functional Analysis and its Applications, vol. 9, pp. 183–185, 1975.
- [6] T. Bogart, A. Jensen, D. Speyer, B. Sturmfels, R. Thomas: *Computing tropical varieties*. Journal of Symbolic Computation, vol. 42(1), pp. 54–73, 2007.
- [7] R. Descartes: *La géométrie*. 1637.
- [8] S. Evans: *The expected number of zeros of a random system of p-adic polynomials*. Electron. Comm. Probab., vol. 11, pp. 278–290, 2006.

- [9] A. Khovanskii: *Fewnomials*. AMS Press, Providence, Rhode Island, 1991.
- [10] H.W. Lenstra: *On the Factorization of Lacunary Polynomials*. Number Theory in Progress, vol. 1, pp. 277-291, 1999.
- [11] B. Poonen: *Zeros of sparse polynomials over local fields of characteristic p* . Math. Res. Lett., vol 5(3), pp. 273-279, 1998.
- [12] J. Richter-Gebert, B. Sturmfels, T. Theobald: *First steps in tropical geometry*. Contemporary Mathematics, vol. 377, pp. 289–317, 2005.
- [13] A. Robert: *A course in p -adic Analysis*. GTM, Vol.198, Springer-verlag, 2000.
- [14] J.M. Rojas: *Arithmetic Multivariate Descartes' rule*. American Journal of Mathematics, vol. 126(1), pp. 1–30, 2004.
- [15] D. Speyer, B. Sturmfels: *The tropical Grassmanian*. Advances in Geometry, vol. 4, pp. 389–411, 2004.